

VACMAN Controller for HSM

Integration Guideline

Disclaimer

Disclaimer of Warranties and Limitation of Liabilities

All information contained in this document is provided 'as is'; VASCO Data Security assumes no responsibility for its accuracy and/or completeness.

In no event will VASCO Data Security be liable for damages arising directly or indirectly from any use of the information contained in this document.

Copyright

© VASCO Data Security 2006. All rights reserved.

Trademarks

DIGIPASS and VACMAN are trademarks of VASCO Data Security. All other trademarks are trademarks of their respective owners.

Table of Contents

VACMAN Controller for HSM.....	1
Disclaimer	2
Table of Contents.....	3
1 Introduction.....	4
1.1 Background.....	4
1.2 Supported HSM Models	4
1.3 Glossary	4
1.4 Target Audience.....	5
2 HSM Integration Architecture	6
2.1 General	6
2.2 HSM Independence.....	6
2.3 Operating Modes	6
2.3.1 <i>Data Encryption Only</i>	7
2.3.2 <i>Data Encryption and DES Operations</i>	8
2.3.3 <i>Data Encryption, DES Operations and VC Operations</i>	9
3 VACMAN Controller for HSM – Additional Features.....	10
3.1 DPX Double Encryption	10
3.2 HSM Storage Key Migration	11
3.3 HSM Load Balancing and Fail Over	11
3.4 HSM Key Names and Identifiers.....	12
4 Additional information	12
5 About VASCO.....	12

1 Introduction

1.1 Background

The VACMAN Controller allows the verification of passwords and signatures generated by a Digipass. To verify these passwords, the VACMAN Controller needs access to the parameters and secrets that were programmed in the Digipass. The VACMAN Controller will store this information in what is called the Digipass Blob. The Digipass Blob is a flat data structure that must be stored in the Application Database on the Host computer that runs the VACMAN Controller.

To prevent fraud from people having access to the database, the Digipass Blob is protected (privacy and integrity) with a 3DES-based encryption.

The standard VACMAN Controller uses a Software Security Module (SSM). This means that the Digipass Keys used in the VACMAN Controller verification process are encrypted by (1) secret codes stored in the software; and (2) secret codes passed during run-time. In the standard implementation of VACMAN Controller, these Digipass Keys are therefore, at some point during the verification process, exposed on the Application Host.

Benefits of HSM implementation

In case a higher level of security is required, or to benefit from an existing architecture, it is possible to use the "VACMAN Controller for HSM" solution.

A Hardware Security Module (HSM) is a tamper-proof hardware device that is connected to, or inserted into the Application Host.

A HSM facilitates secure long-term storage for cryptographic keys, in combination with cryptographic processing capabilities. Typically a HSM Storage Key is used to encrypt the Digipass Keys that are used to authenticate users and transactions. The encrypted Digipass Keys remain in the Digipass Blob and stored in the Application Database.

NOTE: The Digipass Blobs and the Digipass Keys are NOT stored in the HSM – only the HSM Storage Keys (and HSM Transport Keys) are stored in the HSM.

Using a HSM in combination with the VACMAN Controller guarantees that Digipass Keys are never exposed on the Host computer.

1.2 Supported HSM Models

The VACMAN Controller currently integrates with 4 different HSM models – **nCipher**, **Eracom**, **Thales** and **ICSF**.

1.3 Glossary

Below are terms specific to the VACMAN Controller for HSM integration.

Application Host The back-end/host system where the user and transaction authentication takes place.

Digipass Blob See Digipass Data.

Digipass Data	Digipass Data contains information about a particular Digipass that is stored in the customer's application database and used in the VACMAN Controller verification process. This includes Digipass Key(s).
Digipass Key	Cryptographic key stored both in the Digipass and in the Digipass Blob. It is used to generate One Time Passwords and Signatures using cryptographic algorithms.
Digipass	Digipass is a Hardware device or Software instance that is used to generate One Time Passwords and Signatures.
DPX file	A flat ASCII file that contains the Digipass Data for each Digipass in a particular batch. The Digipass Keys inside this file are encrypted.
HSM	Hardware Security Module - a tamper-proof hardware device with cryptographic capabilities.
HSM Storage Key	Key stored in HSM and used long-term to encrypt/decrypt Digipass Keys.
HSM Transport Key	Key stored in HSM and used to encrypt the Digipass sensitive information inside the DPX file before the DPX file is sent from VASCO to the customer. This requires that VASCO receives this HSM Key from the customer. The name of the HSM Transport Key, used to encrypt the Digipass Keys during the transport, will be stored in the DPX file.
Integrator	The company/engineer that is responsible to integrate VACMAN Controller into the application.
KCV	Key Check Value – created and stored in the DPX file to ensure the HSM Transport Key name has not been corrupted.
KEK	Key Encryption Key – used to encrypt the HSM Transport Key before transferal from customer to VASCO.
VC	VACMAN Controller

1.4 Target Audience

This document is designed to assist VASCO customers and partners who are interested in integrating VACMAN Controller into their application. It will allow them to make the necessary choices with regards to the integration of the VACMAN Controller with a specific HSM.

2 HSM Integration Architecture

2.1 General

The VACMAN Controller for HSM solution has been engineered so that it utilizes the general features of a HSM, as well as giving the customer the opportunity to integrate VACMAN Controller into an existing or new application in a smooth way.

2.2 HSM Independence

VACMAN Controller for HSM is provided with a level of HSM independence. That is to say, the VC library is a set of functions that give integrators simplified HSM support without the restriction of conforming to one particular HSM model. This will allow the simplest integration scenario – development will focus on application instead of HSM compliance.

On the Host, VACMAN Controller does not perform any HSM Management processes (i.e. initialization/finalization, session management, communication). Integrators write this functionality separately from VACMAN Controller, in line with the particular HSM in use.

VACMAN Controller provides the Host-side generation/processing of the messages sent to/from the HSM. In this way, there is a complete separation of VACMAN Controller and HSM Management processes.

For each VACMAN Controller function performed inside the HSM, the Host-side VACMAN Controller must perform:

- Generation of a HSM Command message to be sent from the Host to the HSM.
- Processing of the HSM Reply message that is sent back from the HSM.

Note that due to this separation of tasks, integrators must have knowledge of the operation and management of their HSM.

2.3 Operating Modes

The customer must decide which operating mode to use. The choice may be limited if a particular HSM is already in place or a mainframe is used.

There are 3 operating modes:

1. **Data Encryption Only** – supported by IBM® ICSF® systems.
2. **Data Encryption and DES Operations** – supported by any PKCS#11 compliant HSM.
3. **Data Encryption, DES Operations and VC Operations** – supported by nCipher and Eracom HSM's.

2.3.1 Data Encryption Only

In this operating mode, the HSM is simply used to store HSM Storage Keys and to encrypt and decrypt the Digipass Keys. The DES operations and OTP validation will be processed by the Vacman Controller software that is running on the Application Host.

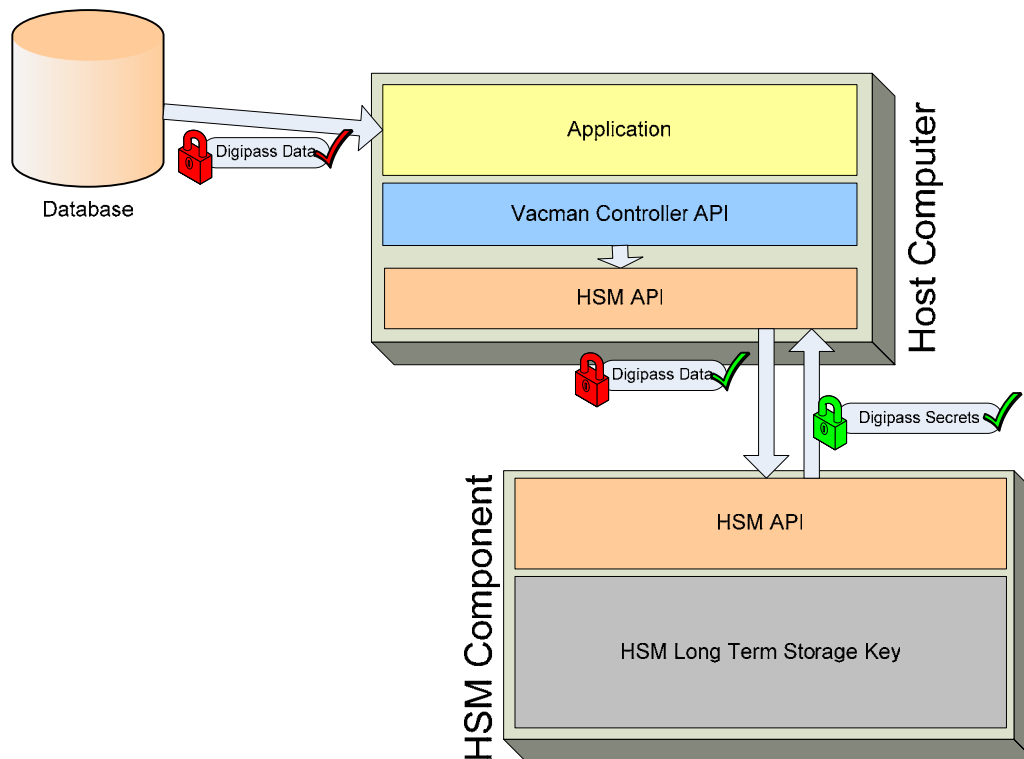


Figure 1 - Data Encryption Only architecture

With this mode we ensure that no one can use the Digipass Data except the Application Host that has access to the HSM.

1. First the application retrieves the relevant Digipass Data record from the database. Here, the Digipass Data is secured by HSM Storage Key encryption (lock) and VC Software integrity (tick).
2. The VACMAN Controller calls the HSM API with the encrypted Digipass Data.
3. A HSM session is established and Digipass Keys in the Digipass Data are decrypted and returned.
4. The VACMAN Controller uses the Digipass Keys to perform 3DES and OTP validation.

This VACMAN Controller for HSM Operating Mode is in use with the IBM® ICSF® system.

2.3.2 Data Encryption and DES Operations

With this operating mode, not only the secrets are in the HSM, but also the DES or other cryptographic processing is done inside the HSM itself.

The result of the cryptographic operation won't be accessible by any process outside the HSM. Output will be a cryptogram that the VACMAN Controller will use to verify a One-Time Password or Signature code.

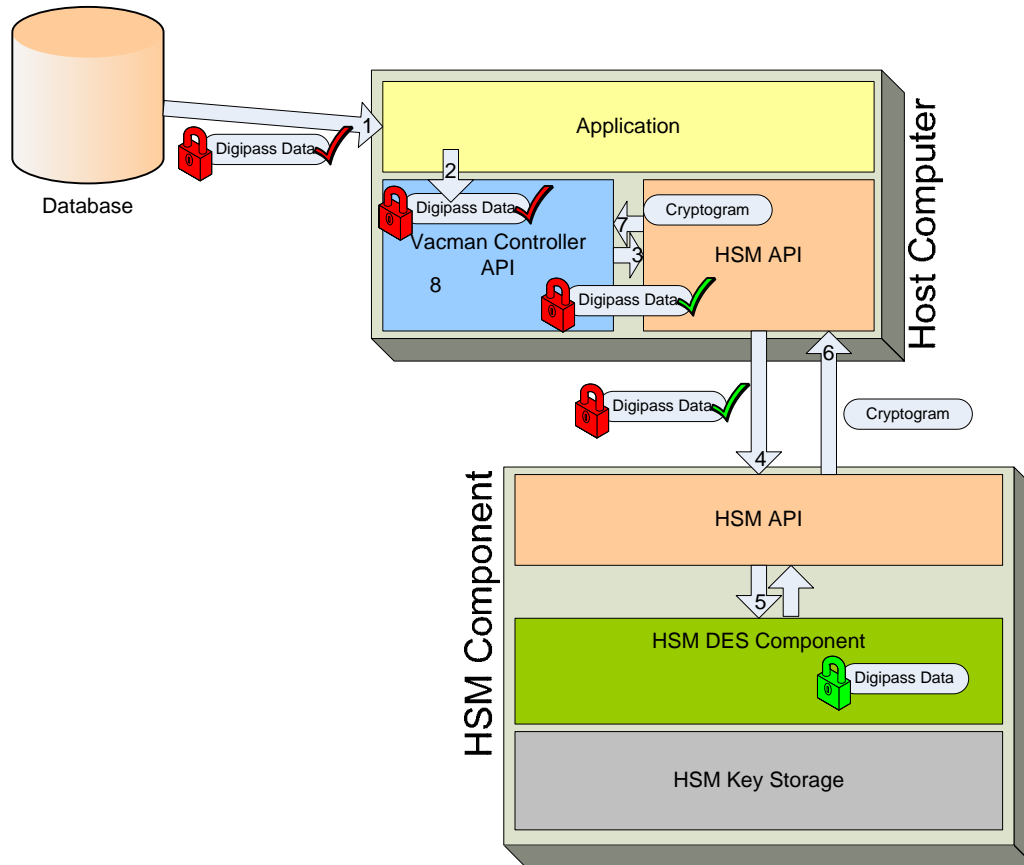


Figure 2 - Data Encryption and DES Operations architecture

1. First the application retrieves the relevant Digipass Data record from the database. Here, the Digipass Data is secured by HSM Storage Key encryption (lock) and VC Software integrity (tick).
2. The application calls a VC API, passing the Digipass Data to the VACMAN Controller (Software). The Digipass Data is checked for integrity (Hash calculation).
3. The Digipass Data, containing the encrypted Digipass Key, is sent to HSM API along with HSM Storage Key name and the input of the DES.
4. The HSM API connects to the HSM and provides it with this information.
5. The Digipass Key is then decrypted with the HSM Storage Key and the cryptographic (e.g. DES) calculation is performed by the HSM. (The Digipass Key does not leave the HSM in clear).
6. The HSM returns the cryptogram (result of the cryptographic operation) to the Host side HSM API.

7. The HSM API provides the VACMAN Controller (Software) with the Cryptogram.
8. The VACMAN Controller (Software) will use this cryptogram to generate a Dynamic Password to match the one provided by the application (the end user).

With this operating mode, you ensure that not only the Digipass Keys are secure, but also that no process on the Application Host has access to the result of cryptographic operations. This VACMAN Controller for HSM Operating Mode can be applied on any PKCS#11 compliant HSM. It is in use with the Thales HSM. The main disadvantage of this approach is that the validation of a Digipass password or signature may require several communications with the HSM, this for each DES/3DES calculation that needs to be performed.

2.3.3 Data Encryption, DES Operations and VC Operations

This mode will need a specific integration in the HSM – the VACMAN Controller for HSM will reside in the HSM, depending on the vendor prerequisites.

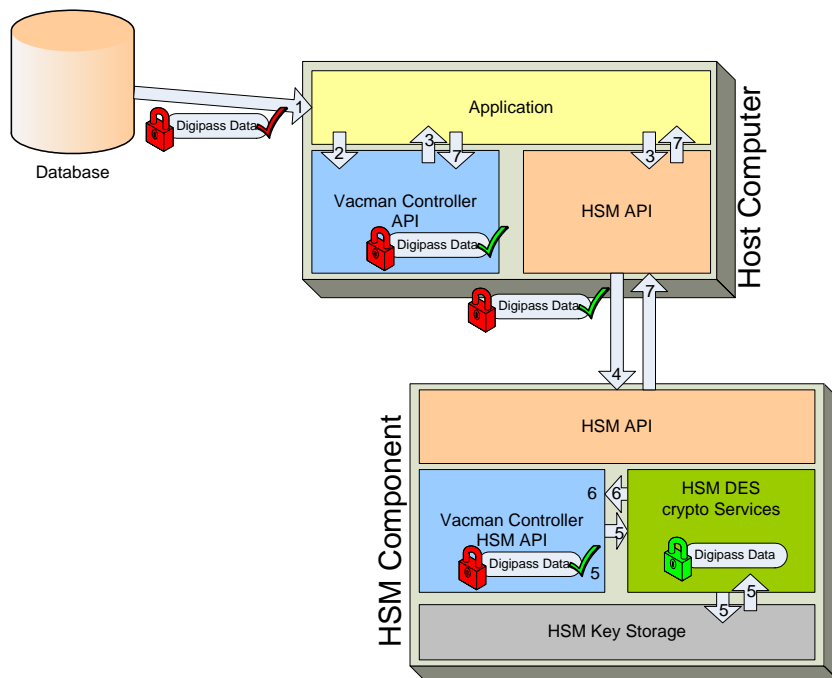


Figure 3 - Data Encryption, DES Operations and VC Operations

1. First the application retrieves the relevant Digipass Data record from the database. Here, the Digipass Data is secured by HSM Storage Key encryption (lock) and VC Software integrity (tick).
2. The Digipass Data is passed to the VACMAN Controller (Software part) to be checked for integrity (Hash calculation).
3. The Digipass Data and Operation Request (e.g. OTP Verification) are formatted, serialized into a Command Message. This Command Message is sent to the HSM API (via the Application) along with credentials if needed.
4. The HSM API connects to the HSM and provides it with the Command Message.

5. The Requested Operation is then performed after another integrity check on the Digipass Data.
6. The VACMAN Controller HSM API has a handle to use the Digipass Data (but not to read it) and perform OTP Verification.
7. The VACMAN Controller for HSM API creates a Reply message. This includes updated Digipass Data and a Operation Success Status code. The reply is provided back to the Software Vacman Controller via the application and the HSM API's.
8. The Software VACMAN Controller uses the handle to Digipass Data to update it and pass it to the application (that will store it in the database).

With this operating mode, the HSM acts as a 'black box' where the critical authentication process is heavily protected. Already, nCipher (nShield and netHSM models) and ERACOM Protect Orange are supported.

3 VACMAN Controller for HSM – Additional Features

3.1 DPX Double Encryption

The DPX file generation process can be modified so that the Digipass Keys are first encrypted by a HSM Transport key. The encrypted Digipass Keys are embedded in the DPX file and additionally encrypted in the standard DPX way, using a software security module (Software level Transport Key).

As a result, the Digipass Keys in the DPX are double encrypted and the remaining data single encrypted.

The purpose of this is to assure the Digipass Keys on the Application Host are continuously secured by HSM-level encryption (Transport or Storage Key) - the Digipass Keys will never be exposed during this process.

When importing the DPX file, the DPX to Digipass Data conversion will be carried out in the normal way, in software. The (software-decrypted) Digipass Data would then contain Digipass keys encrypted under a HSM Transport key.

The AAL2MigrateBlobHSM function is used to decrypt the Digipass Keys using the HSM Transport key and re-encrypt them under the HSM Storage key.

The final Digipass Data is encrypted at the software level. This creates a Digipass Data entirely compatible with the existing VC for HSM integration, using exactly the same double-encryption format for the Digipass Keys inside the Digipass Data.

Modified Import Process

For the VACMAN Controller Integrator, the DPX import process is slightly modified. It is now necessary to add an extra VC API call after retrieving a Digipass Blob – AAL2MigrateBlobHSM. Sample pseudo-code follows below.

```
For each different application name in DPX File Do
  AAL2DPXInit()
  For each Digipass in DPX file with current application name Do
    AAL2DPXGetToken()
    AAL2MigrateBlobHSM()
    Store Digipass Blob in Application Database
  EndFor
  AAL2DPXClose()
EndFor
```

Prior to any password or signature validation it is required that you migrate the Digipass Data encryption in this way. The VACMAN Controller API Authentication and Management functions will reject a Digipass Blob that is encrypted with a HSM Transport key.

HSM Transport Key Import

The HSM Transport Key resides on the customer's HSM. However it must be sent to VASCO before any DPX double encryption process can commence. Standard procedures for this Key transferal are available – the customer must fill out a Request for import of HSM-level DPX Transport Key for Double DPX Encryption form (more detailed information is available upon request).

The actual transfer involves use of a Key Encrypting Key (KEK) – this KEK has previously been created and shared by the customer and VASCO. The KEK is used to encrypt the HSM Transport Key so as to provide a secure means of transferring it.

3.2 HSM Storage Key Migration

To update the HSM Storage Key that is used to encrypt the Digipass Blobs, there is the AAL2MigrateBlobHSM function.

With this function you pass the old and new HSM Storage Key names (or old and new HSM Storage Key ID's). The Digipass Blob now has HSM-level encryption using the new HSM Storage Key. From then on you must pass the new HSM Storage Key to the verification process and other VC functions.

3.3 HSM Load Balancing and Fail Over

The double encrypted Digipass Blobs will be rendered useless if the HSM Storage Key, used to encrypt them, is lost or corrupted, or in the event that the HSM fails. In this case, there are 2 options recommended:

- Provide a backup HSM containing the same HSM Storage Keys.
- Provide secure backup media that will enable you to restore the HSM Storage Keys.

3.4 HSM Key Names and Identifiers

VACMAN Controller uses specific names or ID's for referencing the HSM Storage Key and HSM Transport Key.

Note that you may use any of these names / ID's for either HSM Storage Key or HSM Transport Key.

HSM Key Name	HSM Key ID
vascoStorageKey	0
vascoTransportKey	0x7FFFFFF
vasco1	1
vasco2	2
vasco3	3
vasco4	4
vasco5	5
vasco6	6
vasco7	7
vasco8	8
vasco9	9

4 Additional information

Please refer to the following White Paper - VACMAN Controller Integration.

5 About VASCO

VASCO designs, develops, markets and supports patented user authentication products for the financial world, remote access, e-business and e-commerce. VASCO's user authentication software is delivered via its Digipass hardware and software security products. With over 20 million Digipass products sold and delivered, VASCO has established itself as a world-leader for strong User Authentication with over 440 international financial institutions and approximately 2,300 blue-chip corporations and governments located in more than 100 countries.